

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

REGULATING AI IN INDIA: EXAMINING THE DPDP ACT, 2023 AND THE EMERGING FRAMEWORK FOR RESPONSIBLE AI GOVERNANCE

AUTHORED BY - MITANSHI KHANDELWAL

Abstract

In India, artificial intelligence (AI) is increasingly used in areas such as healthcare, education, banking, employment, public administration and more. While AI holds the promise of greater efficiency and economic growth, it also involves aspects of privacy, discrimination, transparency, and accountability. There is no all-encompassing legislation in India that covers all aspects of artificial intelligence. Rather, its regulatory process is evolving via existing laws such as the Digital Personal Data Protection Act, 2023 (DPDP Act), the Information Technology Act, 2000 and government initiatives on the responsible use of AI. The DPDP Act also remains significant, as numerous AI systems are trained on personal data and use it to make predictions and decisions. But data protection is not enough to deal with every danger posed by AI – from discriminatory outputs and flawed decisions to synthetic content that can be harmful. This paper highlights the significance of the DPDP Act in the current framework of governance of AI in India and sheds light on the shortcomings in the current legal regime. It argues that the Act provides a useful foundation to safeguard personal data but is not a comprehensive blueprint for AI regulation. There should be a coordinated, risk-based approach in India that not only reinforces data protection principles, but also ensures adequate transparency and human oversight, curbs discriminatory practices and offers robust remedies in cases of violations. This should foster innovation whilst at the same time safeguarding constitutional values and individual rights.

Keywords: Artificial Intelligence, Digital Personal Data Protection Act, 2023, AI Governance, Data Protection, Privacy, Algorithmic Accountability, Responsible AI, India.

1. Introduction

AI is playing a significant role in India's digital evolution. Medical information is analysed using AI, fraud detection software uses AI, educational resources are recommended by AI systems, public authorities are assisted with AI, and written, pictorial and auditory content is produced with AI. These can help lower costs and have beneficial implications for access to service provision and economic growth. Yet their growing usage is bringing about legal problems which will not be solved through technological development.

AI systems might utilize private data without individuals understanding how it is collected or used. They can also yield misleading outcomes and perpetuate social inequalities and influence decisions concerning employment, credit, education and access to public services. It may be hard to identify what organisation is responsible for harm when it has taken place and challenging an automated decision.¹

India's response to these concerns has evolved based on laws, policy initiatives, and guidance on responsible AI usage. Personal data plays a significant role in several AI applications, making the DPDP Act 2023 stand out as being of special significance. Also, from the aspect of legislations, the Information Technology Act, 2000 and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 could be relevant to specific AI-related activities, depending on the circumstances.²

The new governance mechanism in India aims to foster creativity while dealing with AI-related risks. But one key issue remains - is the current legal framework effective in protecting people from harm caused by AI?

Drawing on this, this paper proposes a framework that establishes that the DPDP Act offers a crucial basis for regulating AI systems dealing with digital personal data, and that it is insufficient to regulate all harms that may come from the development and deployment of AI. India requires a coordinated, risk-based approach linking data protection, transparency, human oversight, non-discrimination, and adequate legal avenues that is missing today. It should be the goal to seek to identify specific regulatory gaps and without unnecessarily restricting beneficial technological development.

¹ Ministry of Electronics and Information Technology, Government of India, India AI Governance Guidelines (2025).

² Information Technology Act, 2000 (Act No. 21 of 2000); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3–4.

2. The DPDP Act, 2023 and AI Governance

The Digital Personal Data Protection Act, 2023 govern the processing of personal digital data, within its scope. It aims to protect individuals' personal data, while still allowing it to be processed legally. It matters to AI with regard to training, testing, and personalisation of AI systems as well as automated analysis of personal information.

The Act distinguishes between a Data Principal (whose personal data is being processed) and a Data Fiduciary (who decides upon the purposes and the means of the personal data processing) and a Data Processor (who processes personal data on behalf of the Data Fiduciary). It is important that these differences exist because several organisations may be involved in the development of AI.

For instance, one company could create the AI tool to organize recruiting, another organization could offer the technology for implementing the tool, and an employer could use the tool to evaluate prospective employees. Their responsibilities depend on their respective roles and the respective rules of law. The Data Fiduciary is not automatically exempt from its responsibilities by outsourcing technical processing.³

The Act does not introduce an all-encompassing system of approvals or licences for all AI models. Rather, it regulates covered processing of digital personal data. Therefore, it is dependent on the kind of data, purpose of processing and legal responsibilities of the parties.

Consent, lawful processing and data security

Consent is an important element of the DPDP Act. If consent is being relied upon, it must meet all the requirements prescribed by law, namely, it must be free, specific, informed, unconditional and unambiguous and it must include a clear affirmative action. The Act also outlines some legitimate uses of personal data that are not reliant on consent to the same extent. These provisions do pose key questions to be addressed in the context of developing AI. Personal data collected for one purpose could later be used for another purpose for a different model or product. An organisation may not assume that the original collection constitutes blanket permission to use the material for any purpose following the collection. It should assess whether the proposed processing is covered by valid consent or another applicable legal basis.⁴ Consider, for instance, an educational platform that collects student data through online courses, which then aims to create a predictive system in order to predict students' academic

³ Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), ss. 2(i)–(k), 8(1).

⁴ Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), ss. 4–7.

performance. The legality of this supplementary processing shall be judged on the basis of the rules contained in the Act.

But consent will not prevent all issues with AI. Individuals may not understand how their personal data may influence future decisions. At times, they may not have a realistic option in using an essential service. Therefore, organisations are urged to supply clear details regarding uses of data and should not view consent as a substitute for responsible system design.

The Act also imposes requirements for implementing reasonable security measures and for the accuracy and completeness of personal data in specific cases, as well as a requirement to tackle personal data breaches. The obligations apply to situations where AI systems store, analyse or exchange personal information.⁵

Regarding the reliability of assessment, poor data quality can lead to unreliable assessments, on the other hand with the lack of security it can expose personal information to unauthorised access. Appropriate steps must be taken to protect data and comply with applicable laws. However, data correctness and security do not ensure fair and reliable results for an AI system. Data protection mitigates significant risks, but in no way solves issues resulting from the design or use of an algorithm.

Individual rights and accountability

The DPDP Act includes rights of Data Principals which cover, inter alia, rights to information relating to personal data, rights to the correction, completion, updating and erasure of personal data, rights to erasure, rights to a remedy with respect to complaints and rights to a nominee, on condition and subject to exceptions. The rights can assist a person whose personal data is processed by an AI system.⁶

Correcting personal data and challenging an AI decision are different matters. But fixing a record that is inaccurate might not eliminate bias in a credit assessment model. Likewise, the right to information regarding the processing of his or her own information should not be interpreted as a universal right to access the source code or a full technical explanation of every AI output.

The Act sets up the Data Protection Board of India and provides for penalties for specified contraventions. These mechanisms can help increase accountability when the data-protection obligations are not fulfilled. Implementation and institutional capacity and access to complaint mechanisms will affect their effectiveness.

⁵ Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), s. 8(3), (5)–(6).

⁶ Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), ss. 11–14.

Mainly, the Act does not lack relevance on AI. Instead, its statutory intent is more limited than the spectrum of risks that are posed by an AI system. Such a system may be compliant with applicable data-protection requirements and yet yield discriminatory outcomes or may generate misleading content or make inappropriate recommendations. These issues may require additional legal safeguards.

3. India's Emerging Framework for Responsible AI

India's vision for AI governance goes far beyond data protection. The IndiaAI Mission and the India AI Governance Guidelines highlight a commitment to foster the advancement of AI within the limits of safety, fair access, accountability, and public trust.⁷

The principles featured in the India AI Governance Guidelines include putting people first, fairness and equity, accountability, understandability by design, and safety and resilience. There is a case to promote proportionate dealing with the risks of AI, not as if all uses are equal. This is an important method for two reasons: First, AI systems have great variability in their impact. The risks associated with a tool that recommends music are different from those if the tool were used to judge job applicants or to decide who is eligible for publicly funded services. Regulation should be consistent with the purpose of the system, seriousness of any potential harm and who it will impact.

The guidelines also recognise the need for inter-agency, regulatory, technical and industry coordination. This type of coordination can be used to fill the regulatory gaps and to better assess complex systems. But policy guidelines are not legislation. While their recommendations are important, they do not necessarily have the effects of an Act of Parliament or valid statutory rules and obligations.⁸

The Union Cabinet approved the IndiaAI Mission in March 2024 to enable the development of AI capability in India by providing support for developing computing infrastructure, domestic innovation, and skills and related initiatives. Its Safe and Trusted AI component, which aligns with the risks associated with AI technology, is relevant for AI risk identification and mitigation.

Such efforts demonstrate the development aspects of governance as well as the risk management aspects of AI governance. While the technical advancements of AI can be

⁷ Ministry of Electronics and Information Technology, Government of India, India AI Governance Guidelines (2025); Press Information Bureau, Government of India, Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem (7 March 2024).

⁸ Ministry of Electronics and Information Technology, Government of India, India AI Governance Guidelines (2025).

harnessed to develop applications that address the needs of local language and socio-cultural contexts, it is essential that these developments are supported by appropriate legal and institutional measures. Regulators must have the ability to assess reliability, security, and discriminatory aspects.

AI specific issues are further addressed by Information Technology Act, 2000 and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Examples of this include potential legal issues related to impersonation, fraud, privacy, or illegal online activity. A particular provision applies only when the relevant statutory conditions are satisfied.⁹

Current digital laws can only cover specific types of harms but are not necessarily tailored to provide a comprehensive regime for assessing the design, safety, and fairness of AI systems before they are introduced into the market. India should identify specific regulatory gaps and address them through targeted measures, rather than assuming that existing laws address every problem or that every new AI application requires separate legislation.

4. Constitutional Principles and AI Regulation

AI regulation must take account of constitutional principles, particularly privacy, equality and individual liberty when considering AI regulation.

The Supreme Court, in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), recognised the right to privacy as a fundamental right. The decision matters because AI systems can collect, combine and analyse personal information to infer about an individual's behaviour, personal preferences, and situations.¹⁰

But privacy issues are not limited to the "public disclosure of personal information". The processing of personal data for the purpose of profiling the persons or forecasting their behaviour could also have adversely affected their autonomy and freedom. However, these elements of the constitutional right to privacy are not all the same as are contained in the statutory protection conferred under the DPDP Act. The Act regulates covered processing of digital personal data and the constitutional principles are relevant to the exercise of public power and can guide the interpretation of applicable laws.

Another key consideration is equality. The equality before the law and the equal protection of the laws are guaranteed in article 14 of the Constitution. Article 15 prohibits specified forms

⁹ Information Technology Act, 2000 (Act No. 21 of 2000); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3–4.

¹⁰ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

of discrimination by the State, subject to the constitutional text and its exceptions. AI systems deployed by public bodies could have constitutional concerns when they lead to arbitrary or discriminatory treatment.¹¹

For instance, let us say an automated system to prioritize applications for a welfare scheme is based on the wrong criteria or on data that is biased, it may disadvantage a particular group of applicants. It is possible that this could be a violation of the constitution if the facts support that assertion and the laws in effect apply.

The position is more complex for private organisations that manage the use of AI systems. The fundamental rights do not automatically apply in the same way in private disputes as they apply to State action. However, statutory obligations and other forms of legal remedies might continue to be applicable.

The principles highlight that AI governance should involve considerations for protecting citizens as data subjects as well as citizens participating in social and economic life. Equality, fairness, and access to remedies must be part of the look to the regulation, in addition to privacy protection.

5. Major Legal Challenges in Regulating AI in India

Limits of data protection and algorithmic discrimination

The DPDP Act's key limitation is that it addresses covered processing of digital personal data, not every type of harm associated with AI. An AI system may generate false information, make unreliable predictions or produce discriminatory results without every such outcome constituting a violation of data-protection law. A non-personal data system also could cause safety or security issues.¹²

Algorithmic discrimination is challenging. AI systems can develop patterns based on training data and potentially replicate existing inequalities. Bias can also arise from unrepresentative data, discrimination in past decisions or using inappropriate measures.

For instance, a recruitment system using historical hiring decisions could be biased towards applicants with profiles that are similar to the profiles of past hires. In some cases, the system does not expressly use a protected characteristic, and other variables can create patterns of exclusion.

Discrimination must not be the only issue looked at; the legal response should take into account the actual effect as well as purpose and applicable law of the system. India will create suitable

¹¹ The Constitution of India, arts. 14–15.

¹² Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), s. 3.

ways of evaluating the impact of high impact AI systems such as assessing the effect of the AI for discrimination or documenting the basis of consequential decisions.

Transparency and accountability

Ordinary users may have a hard time understanding the results a complex AI system may provide. This can be a serious issue if their decisions affect employment, credit, education or access to public services.

Disclosure of source code is not always a part of transparency. It should, however, be capable of helping affected people and regulators to grasp how AI is being used and to go through established processes to flag major inaccuracies or errors. Since the DPDP Act does not provide a general requirement for a full technological explanation of all the outputs of an AI system, this may be needed in some high-impact applications.

As with projects involving multiple organisations for development and deployment, accountability is also difficult. Different developers, suppliers, and service providers roles can be used. In the event of harm, every party may attempt to pass the blame to another party.

So, in terms of relationships, roles, control, contribution to the harm, and legal responsibilities, there should be a sharing of responsibility. Organisations should not be able to evade responsibility simply by stating that the outcome was generated using an automated system. Meanwhile, responsibility should be assigned appropriately, in line with what happened and not on any of the participants.

Deepfakes and access to remedies

It is important to note that Generative AI can produce realistic images, videos, spoken content, and written content. While these tools are used for legitimate purposes, they may be used to allow for impersonation, fraud, reputational harm, and dissemination of false information.

Examples of this could be when deepfakes depict people in fabricated scenarios or manipulate their speech without the consent of the person depicted. The steps taken in a legal context should identify legitimate creative expression from illegal activity, paying attention to the rights involved, how the activity is being distributed, and the duties of those involved.¹³

Harm can be minimised through appropriate disclosures, content-authentication methods, and complaint procedures. But the restrictions need to be thoughtfully structured to ensure that legitimate expression and uses of synthetic media are not unduly restricted.

¹³ Ministry of Electronics and Information Technology, Government of India, India AI Governance Guidelines (2025).

There's growing worry that enforcement will not be an issue. People might not have the expertise or information to dispute an AI decision. In addition, small companies or public institutions may be short of resources to evaluate complex systems. India should, therefore, increase the level of expertise in the regulatory agencies, public awareness, and ensure accessible complaint mechanisms, with the presence of fair procedures and adequate safeguards for personal or private information.¹⁴

6. Towards a More Effective AI Governance Framework

A coherent and risk-based strategy should be established within India focusing on existing legislation and targeted protection measures as required. Rather than one unified AI statute, the paramount goal needs to be to pinpoint weaknesses and ensure that enforcement is clear and effective.

First, AI applications must be evaluated on the basis of the potential impact. Applications used in consequential decisions concerning employment, credit, essential services or public administration might need more safeguards than other low-risk applications. A risk classification should take into account the purpose to which the product is applied, the people likely to be affected by the system and the seriousness of the potential harm. This could enable regulators to address significant risks while avoiding excessive regulations for regular uses of AI.

Secondly, clear guidance is needed on AI processing of personal data in implementation of the DPDP Act and the Digital Personal Data Protection Rules, 2025. The Digital Personal Data Protection Rules, 2025 were notified on 14 November 2025, with commencement scheduled in phases. As of October 2026, the Act's substantive provisions in Sections 3–17 are scheduled to commence on 13 May 2027. This assessment needs to be undertaken based on the provisions in force at the relevant time as part of their application. Organisations must identify their purposes for processing, comply with their legal obligations and implement appropriate security measures.¹⁵

Thirdly, appropriate procedural safeguards should be introduced for high impact AI systems. These can be a range of documented risk assessments, testing, meaningful human review, and/or sufficient records to review consequential decisions depending on the application.

¹⁴ Information Technology Act, 2000 (Act No. 21 of 2000), ss. 66C–66D; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3–4.

¹⁵ Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), s. 1(2); Digital Personal Data Protection Rules, 2025, r. 1; Ministry of Electronics and Information Technology, Government of India, Notifications G.S.R. 843(E) and G.S.R. 846(E), 13 November 2025.

Human review should allow reviewers to challenge or reject an AI recommendation. The level of scrutiny should be proportionate to the risk.

Four, individuals should be able to understand and challenge decisions that significantly affect them. Organisations should communicate, where appropriate, when AI has had a significant influence in a decision, establish complaint mechanisms and rectify any significant errors by appropriate means. Responsibilities should be allocated according to the roles of developers, providers and deploying organisations.

Last but not least, regulatory policy must not stifle innovation while safeguarding the interests of vulnerable groups. There are opportunities for researchers and businesses to create effective applications through technical guidance, regulatory sandboxes, and proportionate compliance requirements. But do not presume organisations will be excused from complying with the law merely by participating in a testing programme. Likewise, AI systems should be assessed for their suitability in relevant social contexts and across all Indian languages.¹⁶

These measures would link data protection and more general issues of safety, fairness, and accountability concerns. They would also enable to prevent two extremes, namely unnecessary limits in useful technologies and the reliance on “gentle” agreements in the case of necessary technology safeguard.

7. Conclusion

Although AI offers considerable opportunities for India, the growing use of AI presents legal questions around privacy, equality, transparency, and accountability. The Digital Personal Data Protection Act, 2023 offers a crucial framework by regulating covered processing of digital personal data and laying down obligations and rights applicable to numerous AI applications. But there is a statutory scope to the Act. The fulfilment of the data protection standards does not necessarily lead to an accurate, fair, and transparent as well as safe AI system. Discriminatory outcomes, misleading content and inadequate remedies for consequential automated decisions could necessitate other legal and regulatory interventions.

These limitations may be addressed through India’s emerging AI governance framework. The emerging regulatory approach is enhanced by the India AI Governance Guidelines, the IndiaAI Mission and existing information technology laws. Their effectiveness will depend on clearly defined responsibilities, institutional coordination, technical capacity and effective implementation.

¹⁶ Ministry of Electronics and Information Technology, Government of India, India AI Governance Guidelines (2025); Office of the Principal Scientific Adviser to the Government of India, IndiaAI Mission.

Therefore, to ensure that Indian law effectively protects the public interest, it is important for India to reinforce existing law while also introducing additional safeguards for AI applications that pose significant risks. This approach, which balances innovation with the protection of individual rights, can help balance individual rights while avoiding undue limitations on innovation through a mixture of data protection, human oversight, appropriate transparency, and easy remedies.

In summary, AI governance is about how to harness technological advancements without going against constitutional values, accountability and human rights. Developing AI technologies is not enough; people need to be able to trust and challenge the systems that affect their lives for the framework to be a success for India.

